

FORM PTO-1390 US DEPARTMENT OF COMMERCE
REV. 5-93 PATENT AND TRADEMARK OFFICE

**TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371**

ATTORNEYS DOCKET NUMBER

P01,0142

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)

09/831046

INTERNATIONAL APPLICATION NO.

PCT/DE99/03262

INTERNATIONAL FILING DATE

11 OCTOBER 1999

PRIORITY DATE CLAIMED

03 NOVEMBER 1998

TITLE OF INVENTION

METHOD AND ARRANGEMENT FOR AUTHENTICATING A FIRST ENTITY AND A SECOND ENTITY

APPLICANT(S) FOR DO/EO/US

Martin EUCHNER

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of International Application as filed (35 U.S.C. 371(c)(2)).
 - a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3)).
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; (PTO 1449, Prior Art, Search Report, 11 References).
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included.
(SEE ATTACHED ENVELOPE)
13. ☒ Amendment "A" Prior to Action and Appendix "A".
☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☒ A substitute specification and substitute specification mark-up.
15. ☐ A change of address letter attached to the Declaration.
16. ☒ Other items or information:
 - a. ☒ Submission of Drawings
 - b. ☒ EXPRESS MAIL #EL 843728288 US dated May 3, 2001

U.S. APPLICATION NO. (if known, see 37 C.F.R. 1.51)

09/831046

INTERNATIONAL APPLICATION NO
PCT/DE99/03262ATTORNEY'S DOCKET NUMBER
P01,014217. ☒ The following fees are submitted:**BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5):**

Search Report has been prepared by the EPO or JPO \$860.00

International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) \$690.00

No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2)) \$710.00

Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2)) paid to USPTO \$1000.00

International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) \$100.00

ENTER APPROPRIATE BASIC FEE AMOUNT =

CALCULATIONS

PTO USE ONLY

\$ 860.00

Surcharge of \$130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).

\$

Claims	Number Filed	Number Extra	Rate
Total Claims	10 - 20 =	0	X \$ 18.00
Independent Claims	03 - 3 =	0	X \$ 80.00
Multiple Dependent Claims			\$270.00 +

TOTAL OF ABOVE CALCULATIONS =

\$ 860.00

Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)

\$

SUBTOTAL =

\$ 860.00

Processing fee of \$130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)) +

\$

TOTAL NATIONAL FEE =

\$ 860.00

Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31) \$40.00 per property +

TOTAL FEES ENCLOSED =

\$ 860.00

Amount to be
refunded

\$

charged

\$

a. ☒ A check in the amount of \$ 860.00 to cover the above fees is enclosed.b. ☐ Please charge my Deposit Account No. _____ in the amount of \$ _____ to cover the above fees.
A duplicate copy of this sheet is enclosed.c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1519. **A duplicate copy of this sheet is enclosed.**

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

SCHIFF HARDIN & WAITE
PATENT DEPARTMENT
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473

SIGNATURE - MARK BERGNER

(Reg. No. 45,877)

Date: May 3, 2001

CUSTOMER NUMBER 26574

BOX PCT
 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
 OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
 UNDER THE PATENT COOPERATION TREATY--CHAPTER II

PRELIMINARY AMENDMENT A
PRIOR TO ACTION

APPLICANT(S): Martin EUCHNER
 ATTORNEY DOCKET NO.: P01,0142
 INTERNATIONAL APPLICATION NO: PCT/DE99/03262
 INTERNATIONAL FILING DATE: 11 OCTOBER 1999
 INVENTION: METHOD AND ARRANGEMENT FOR
 AUTHENTICATING A FIRST ENTITY AND A SECOND
 ENTITY

Assistant Commissioner for Patents,
 Washington D.C. 20231

Sir:

Applicants herewith amend the above-referenced PCT application, and request entry of the Amendment prior to examination on the United States Examination Phase.

IN THE CLAIMS:

On amended page 12:

replace line 1 with --WHAT IS CLAIMED IS:--;

Please replace original claims 1-8 with the following rewritten claims 1-8, referring to the mark-ups in Appendix A.

1. (Amended) An authenticating method, comprising the steps of:
 carrying out a first operation $A(x,g)$ on a prescribed known value g and on a value x known only to a first entity, said first operation $A(x,g)$ being an asymmetric cryptographic method, thus producing a first operation result;
 encoding said first operation result utilizing a first key, which is known to said first and to a second entity, said encoding being carried out with said first key utilizing a symmetrical encoding method, thus producing an encoded first operation

result, said first operation result being a second code with which said first entity is authorized to undertake a service on said second entity;

transmitting said encoded first operation result by said first entity to said second entity;

5 decoding said encoded first operation result by said second entity with said first key, and the first entity is thereby authenticated;

determining said second key in relation to $G(gxy)$, by said second entity carrying out a second operation $G(gy)$ with a secret number y known only to it;

encoding a result of said second operation with said first key; and

10 transmitting said encoded second operation result to said first entity.

2. (Amended) The method as claimed in claim 1, wherein said first operation $A(g,x)$ is a Diffie-Hellman function ($G(gx)$), $G()$ being an arbitrary, finite cyclic group G ; and said first operation is an RSA function xg .

3. (Amended) The method as claimed in claim 1, wherein said first operation is carried out on a group G selected from the group consisting of:

a) a multiplicative group F_q^* of a finite body F_q , in particular having

- a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p ;
- a multiplicative group F_t^* with $t = 2m$ over a finite body F_t of characteristic 2;

- a group of units Z_n^* with n as a composite integer;

b) a group of points on an elliptic curve over a finite body; and

25 c) a Jacobi variant of a hyperelliptic curve over a finite body.

4. (Amended) The method as claimed in claim 3, wherein said second key is a session key or an authorization associated with an application.

5. (Amended) The method as claimed in claim 1, wherein the Diffie-Hellman method is used to generate said second key.

6. (Amended) The method as claimed in claim 1, wherein said encoding is carried out with said first key utilizing a one-way function.

7. (Amended) The method as claimed in claim 1, wherein said transmitted data are confidential data.

8. (Amended) An authenticating arrangement comprising a processor unit configured to execute the method of claim 1.

Please add the following new claims 9 and 10.

9. (New) The method according to claim 6, wherein said one-way function is a cryptographic one-way function.

10. (New) An authenticating method, comprising the steps of:

carrying out a first operation $A(x,g)$, using a processor of a first entity, on a prescribed known value g and on a value x known only to said first entity, said first operation $A(x,g)$ being an asymmetric cryptographic method, thus producing a first operation result;

encoding said first operation result utilizing a first key, which is known to said first and to a second entity, said encoding being carried out with said first key utilizing a symmetrical encoding method by said processor of said first entity, thus producing an encoded first operation result, said first operation result being a second code with which said first entity is authorized to undertake a service on said second entity;

transmitting said encoded first operation result by said first entity to said second entity via a communication bus connected to said processor of said first entity and connected to a processor of said second entity;

decoding said encoded first operation result by said second entity with said first key using said processor of said second entity, and the first entity is thereby authenticated;


determining said second key in relation to G(gxy), by said second entity carrying out a second operation G(gy) with a secret number y known only to it; encoding a result of said second operation with said first key; and transmitting said encoded second operation result to said first entity via said communication bus.

REMARKS

The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. Pursuant to 37 CFR 1.125 (b), applicants have concurrently submitted a substitute specification, excluding the claims, and provided a marked-up copy. All of the changes are editorial and applicant believes no new matter is added thereby. The amendment, addition, and/or cancellation of claims is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested.

Submitted by,

 (Reg. No. 45,877)
Mark Bergner
Schiff Hardin & Waite
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473
(312) 258-5779
Attorneys for Applicant

CUSTOMER NUMBER 26574

Appendix A Mark Ups for Claim Amendments

This redlined draft, generated by CompareRite (TM) - The Instant Redliner, shows the differences between -

original document : Q:\DOCUMENTS\YEAR 2001\PO10142\ORIGINAL CLAIMS.DOC
and revised document: Q:\DOCUMENTS\YEAR 2001\PO10142\AMENDED CLAIMS.DOC

CompareRite found 47 change(s) in the text

Deletions appear as Overstrike text surrounded by []
Additions appear as Bold-Underline text

1. **(Amended)** An authenticating method, **comprising the steps of:**

carrying [a] ~~in which a first entity carries~~ out a first operation A(x,g) on a prescribed known value g and on a value x known only to [the] ~~a~~ first entity, [the] **said** first operation A(x,g) being an asymmetric cryptographic method, **thus producing a first operation result;**

[b] ~~in which the result of the~~ **encoding said** first operation [is encoded with the aid of] **result utilizing** a first key, which is known to [the] **said** first and to a second entity, [the] **said** encoding being carried out with [the] **said** first key [with the aid of] **utilizing** a symmetrical encoding method, **thus producing an encoded first operation result, said;**

e) ~~in which the result of the~~ first operation [encoded with the first key is transmitted by the first entity to the] **result being a second code with which said first entity is authorized to undertake a service on said** second entity;

[and] **transmitting said encoded first operation result by said first entity to said second entity;**

[d] ~~in which the result of the first~~ **decoding said encoded first** operation [is decoded] **result** by [the] **said** second entity with [the] **said** first key, and the first entity is thereby authenticated;

[e] ~~in which the result of the first operation is a second code with which the first entity is authorized to undertake a service on the second entity;~~

f) ~~in which the second key is determined in relation to~~ G(gxy),

by virtue of the fact that the second entity carries] **determining said second key in relation to G(gxy), by said second entity carrying** out a second operation G(gy) with a secret number y known only to it[, ~~encodes the~~];

encoding a result of [this] **said** second operation with [the] **said** first key [and transmits it to the]; and

transmitting said encoded second operation result to said first entity.

5 2. **(Amended)** The method as claimed in claim 1, ~~[in which the]~~ **wherein** **said** first operation $A(g,x)$ {

a)} is a Diffie-Hellman function $(G(gx))$, $G()$ being an arbitrary, finite cyclic group G ; and **said first operation** $[b]$ is an RSA function xg .

10 3. **(Amended)** The method as claimed in ~~[one of the preceding claims, in which the]~~ **claim 1, wherein said** first operation is carried out on a group G , **selected from** the group ~~[G being one of the following groups]~~ **consisting of:**

- a) a multiplicative group F_q^* of a finite body F_q , in particular having
- a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p ;
 - a multiplicative group F_t^* with $t = 2m$ over a finite body F_t of characteristic 2;
 - a group of units Z_n^* with n as a composite integer;
- b) a group of points on an elliptic curve over a finite body; and
- 20 c) a Jacobi variant of a hyperelliptic curve over a finite body.

25 4. **(Amended)** The method as claimed in ~~[the preceding claim, in which the]~~ **claim 3, wherein said** second key is a session key or an authorization associated with an application.

5 5. **(Amended)** The method as claimed in ~~[one of the preceding claims, in which]~~ **claim 1, wherein** the Diffie-Hellman method is used to generate ~~[the]~~ **said** second key.

6. **(Amended)** The method as claimed in ~~[one of the preceding claims, in which the]~~ **claim 1, wherein said** encoding is carried out with ~~[the]~~ **said** first key ~~[with the aid of]~~ **utilizing** a one-way function~~[, in particular a cryptographic one-way function.]~~.

5

~~[7.]~~7. **(Amended)** The method as claimed in ~~[one of the preceding claims, in which the]~~ **claim 1, wherein said** transmitted data are confidential data.

8. **(Amended)** An authenticating arrangement [in which] **comprising** a processor unit [is provided which is set up in such a way that a method as claimed in one of the preceding claims can be carried out.] **configured to execute the method of claim 1.**

10

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179

This redlined draft, generated by CompareRite (TM) - The Instant Redliner, shows the differences between -

original document : Q:\DOCUMENTS\YEAR 2001\P010142\ORIGINAL SPECIFICATION.DOC
and revised document: Q:\DOCUMENTS\YEAR 2001\P010142\SUBSTITUTE SPECIFICATION.DOC

5

CompareRite found 120 change(s) in the text

Deletions appear as Overstrike text surrounded by []

Additions appear as Bold-Underline text

10

[Description] **SPECIFICATION**

[Method and arrangement for authenticating a first entity and a second entity] **TITLE**

METHOD AND ARRANGEMENT FOR AUTHENTICATING A FIRST ENTITY AND A SECOND ENTITY

15

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The invention relates to a method and an arrangement for authenticating a first entity with a second entity and/or vice versa.

Description of the Related Art

20

[0003] During an authentication, a first entity declares to a second entity reliably that it actually is the first entity. There is a corresponding need in the transmission of (confidential) data to ensure from whom [said] **the** data actually originate.

[0004] A symmetrical encoding method is known from [[1]] **Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-**

25

Verlag, Bergheim 1993, ISBN 3-89238-081-3, (Ruland), pages 42-46. In the symmetric encoding method, a key is used both for the encoding and for the decoding. An attacker who comes into possession of such a key can transform a plain text (the information to be encoded) into encoded text, and vice versa. The symmetrical encoding method is also called private key method or method with a secret key. A known algorithm for symmetrical encoding is the DES (data encryption standard) algorithm. It was standardized in 1974 under ANSI X3.92-1981.

30

[0005] An asymmetrical encoding method is known from [[2]] **Ruland, pages 73-85.** In this case, a subscriber is not assigned a single key, but a key system composed of two keys: one key maps the plain text into a transformed one, while the other key permits the inverse operation and converts the transformed text into plain text. Such a method is termed asymmetric[,] because the two parties participating in a cryptographic operation use different keys (of a key system). One of the two keys, for example a key p, can be made publicly known, if the following properties are fulfilled:

35

[0006] - It is not possible to derive from the key p with a justifiable outlay; a secret key

[0001]

s required for the inverse operation.

[0007] - Even if plain text is transformed with the (public) key p, it is not possible to derive the (secret) key s ~~therefrom~~.

~~from it.~~

5 **[0008]** For this reason, the asymmetric encoding method is also termed a public key method with a key p which can be made known publicly.

[0009] It is possible in principle to derive the secret key s from the public key p. However, this becomes arbitrarily complicated by virtue of the fact, in particular, that algorithms are selected which are based on problems in complexity theory. These algorithms are also spoken of as “one-way trapdoor” functions. A known representative for an asymmetric encoding method is the Diffie-Hellman method ~~[[6]]~~ **A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996, ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524) (Menezes)**. This method can be used, in particular, for key exchange (Diffie-Hellman key agreement, exponential key exchange).

[0010] The term encoding implies the general application of a cryptographic method $V(x,k)$, in which a prescribed input value x (also termed plain text) is converted by means of a secret k (key) into an encoded text $c := V(x,k)$. The plain text x can be reconstructed using knowledge of c and k by means of an inverse decoding method. The term encoding is also understood as “one-way encoding” with the property that there is no inverse, efficiently calculable decoding method. Examples of such a one-way encoding method are {

20 }a cryptographic one-way function or a cryptographic hash function, for example the algorithm SHA-1, see ~~[[4]]~~.

~~[[NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995, available on-line at~~
~~http://csrc.nist.gov/fips/fip180-1.ps.~~

[0011] There is a problem in practice ~~[that it must be ensured]~~ **of ensuring** that a public key which is used to verify an electronic signature really is the public key of the person who is assumed to be the originator of the transmitted data (ensuring the authenticity of the originator). The public key therefore need not be kept secret, but it must be authentic. There are known mechanisms (see ~~[[3]]~~ **Ruland at pages 101-117**) which ensure with a high outlay that the authenticity is reliable. Such a mechanism is the setting up of ~~[what is called]~~ a trust center, which enjoys trustworthiness and with the aid of which general authenticity is ensured. The setting up of such a trust center, and the exchange of the keys from this trust center are, however, very complicated. For example, it must be ensured during the key allocation that it really is the addressee and not a potential attacker who receives the key or the keys. The costs for setting up and operating the trust center are correspondingly high.

35 **SUMMARY OF THE INVENTION**

[0012] It is the object of the invention to ensure authentication~~[, there being no need]~~
without needing to invest in a separate outlay for a certification entity or a trust center.

[0013] This object is achieved ~~[in accordance with the features of the independent patent claims. Developments of the invention follow from the dependent claims.]~~ **according to the discussion below.**

~~[In order to achieve the object, a]~~**[0014] The inventive** method for ~~[authenticating]~~ **authenticating** a first entity with a second entity is ~~[specified,]~~ **provided** in which the first entity {

}carries out an operation $A(x,g)$ on a (publicly) prescribed known value g and on a value x known only to the first entity. The result of the first operation is encoded with the aid of a first key, which is known to the first and second entities. The result of the first operation, encoded by ~~[means]~~ **way** of the first key, is transmitted by the first entity to the second entity.

[0015] It is particularly advantageous in this case ~~[for]~~ **to** use ~~[to be made of]~~ a symmetrical method in order to authenticate one entity in the eyes of a further entity. This authentication is effected without setting up a separate certification entity or a trust center.

[0016] One refinement consists in that the first operation $A(x,g)$ is an asymmetric cryptographic method. In particular, the first operation can be carried out on an arbitrary finite and cyclic group G .

[0017] A further refinement consists in that the first operation $A(x,g)$ is a Diffie-Hellman function $G(gx)$. Alternatively, the first operation can also be an RSA function xg .

[0018] A development consists in that the group G is one of the following groups:

[0019] a) a multiplicative group F_q^* of a finite body F_q , in particular having

[0020] a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p ;

[0021] a multiplicative group F_t^* with $t = 2m$ over a finite body F_t of characteristic 2; **and**

[0022] a group of units Z_n^* with n as a composite integer;

[0023] b) a group of points on an elliptic curve over a finite body; and

[0024] c) a Jacobi variant of a hyperelliptic curve over a finite body.

[0025] A further development consists in that the result of the first operation is a second key with which the first entity is authorized to undertake a service on the second entity.

[0026] An additional refinement consists in that the second key is a session key or an authorization associated with an application.

[0027] It also is a development for the second key to be determined in relation to

[0028] $G(gxy)$,

[0029] by virtue of the fact that the second entity carries out an operation $G(gy)$ with a secret number y known only to it. The result of this second operation is encoded with the first key and

transmitted to the first entity.

[0030] An additional development consists in that the Diffie-Hellman method is used to generate the second key.

[0031] Another refinement consists in that the encoding is carried out with the first key with the aid of a one-way function, in particular a cryptographic one-way function. A one-way function is distinguished in that it is easy to calculate in one direction, ~~[whereas]~~ **but** its inversion can be performed only with so large an outlay that ~~[this possibility can be neglected in practice]~~ **it is impractical**. An example of such a one-way function is a cryptographic hash function which generates an output B from an input A. The output B cannot be used to infer the input A, even when the algorithm of the hash function is known.

[0032] Another development is that the encoding which is carried out with the first key corresponds to a symmetrical encoding method.

~~[Finally, it is a]~~ **[0033]** A final development **is** that the transmitted data are confidential data.

[0034] Furthermore, to achieve the object, an authenticating arrangement is specified in which a processor unit is provided which is set up in such a way that

[0035] a) a first entity can carry out a first operation $A(x,g)$ on a prescribed known value g and on a value x known only to the first entity;

[0036] b) the result of the first operation can be encoded with the aid of a first key known to the first and to a second entity;

[0037] c) the result of the first operation encoded with the first key can be transmitted by the first entity to the second entity; and

[0038] d) the result of the first operation is decoded by the second entity with the first key, and the first entity can thereby be authenticated.

[0039] This arrangement is particularly suitable for carrying out the method according to the invention or one of its developments explained above.

Brief Description of the Drawings

[0040] Exemplary embodiments of the invention are illustrated and explained below with the aid of the ~~[drawing.]~~ **drawings**.

~~[In the drawing:]~~

~~Fig. 1 shows a sketch]~~ **[0041]** **Fig. 1 is a block diagram** relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case;

[0042] Fig. 2 ~~[shows a sketch]~~ **is a block diagram** in accordance with fig. 1 and using the DES algorithm; and

[0043] Fig. 3 ~~[shows]~~ **is a block diagram of** a processor unit.

DETAILED DESCRIPTION OF THE INVENTION

[0044] Fig. 1 is a ~~[sketch]~~ **diagram** relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case. An entity A 101 selects a random number x in a body "mod $p-1$ " (see block 103). The entity 101 now sends an entity 102 a message 104 which has the following format:

[0045] $g, p, T_A, ID_A, g^x \bmod p, H(g^x \bmod p, \text{[PW]} \text{ pw}, ID_A, T_A, \dots),$

[0046] where

x denotes a secret random value of the entity A 101,

y denotes a secret random value of the entity B 102,

g denotes a generator according to the Diffie-Hellman method,

p denotes a prime number for the Diffie-Hellman method,

T_A denotes a time stamp of the entity A during generation and/or transmission of the message,

T_B denotes a time stamp of the entity B during generation and/or transmission of the message,

ID_A denotes an identification feature of the entity A,

ID_B denotes an identification feature of the entity B,

$g^x \bmod p$ denotes a public Diffie-Hellman key of the entity A,

$g^y \bmod p$ denotes a public Diffie-Hellman key of the entity B,

$\text{[PW]} \text{ pw}$ denotes a shared secret between the entities A and B (password "shared secret"),

$H(M)$ denotes a cryptographic one-way function (hash function) over the parameters M , and

$\text{[KEY]} \text{ key}$ denotes a session key common to the two entities A and B.

[0047] If this message has arrived at the entity 102, a random number y is selected there (see block 105) from the body "mod $p-1$ " and a common key is agreed to in a block 106 as

$\text{[KEY]} \text{[0048]} \text{ key} = g^{xy} \bmod p.$

[0049] The second entity 102 transmits a message 107 with the format

[0050] $T_B, ID_B, g^y \bmod p, H(g^y \bmod p, \text{[PW]} \text{ pw}, ID_B, T_B, \dots)$

[0051] to the first entity 101. The first entity 101 will ~~[thereupon]~~ then carry out the operation

$\text{[KEY]} \text{[0052]} \text{ key} = g^{xy} \bmod p$

[0053] in a step 108, this likewise yielding the common key $\text{[KEY-]} \text{"key"}.$

~~[It may be pointed out expressly in]~~**[0054]** In this case ~~[that]~~, for example, the body "mod p-1" has been selected as one of many possibilities. Furthermore, the messages 104 and 107 are ~~[to be]~~ regarded in each case as one possibility of many. In particular, the fields for addressing within the messages depend on the application and/or the transmission protocol used.

5 **[0055]** A cryptographic one-way hash function H is used in ~~[fig]~~ **Fig. 1**. An example for transmitting such a one-way hash function is the SHA-1 algorithm (compare ~~[[4]]~~) **NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; available on-line at <http://csrc.nist.gov/fips/fip180-1.ps>**. The use of a symmetrical encoding method, for example the DES algorithm ~~[[5]]~~ **NIST, FIPS PUB 81: DES Modes of Operation, December 1980; available on-line at**

10 **<http://www.itl.nist.gov/div897/pubs/fip81.htm>**, instead of the one-way hash function H, is illustrated in ~~[fig]~~ **Fig. 2**. The blocks 101, 102, 103, 105, 106 and 108 are identical in ~~[fig-]~~ **Fig. 2** to ~~[fig-4]~~ **Fig. 1**. The message 201 transmitted by the first entity 101 to the second entity 102 has the format

[0056] $g, p, T_A, ID_A, g^x \bmod p, [ENCPW(gx)]$ **Encr_{PW}(g^x mod p, [PW] pw, ID_A, T_A, ...),**

[0057] where

15 ~~[ENCPW(M)]~~**[0058]** **Encr_{PW}(M)** denotes a symmetrical method for encoding the parameter M with the key PW.

[0059] In the reverse direction, the entity 102 sends the entity 101 in fig. 2 the message 202 which has the following format:

[0060] $T_B, ID_B, g^y \bmod p, [ENCPW(gy)]$ **Encr_{PW}(g^y mod p, PW, ID_B, T_B, ...).**

20 ~~[It may be remarked here, in particular, that in]~~**[0061]** In each case, one message (the message 104 in ~~[fig]~~ **Fig. 1**, and the message 201 in ~~[fig]~~ **Fig. 2**) suffices in order to authenticate the first entity 101 with respect to the second entity ~~[202]~~ **102**. Disregarding the fact that the second entity 102, for example, a service to be undertaken within a network connection, ~~[,]~~ ~~[for example the Internet,]~~ must also be authenticated, it can suffice if only the first entity 101 is authenticated. This already ~~[obtains]~~ **derives** after transmission of the respective first messages 104 and 201. If, in particular, the first entity 101 dials in at the second entity 102, it is frequently to be assumed that this second entity 102 is also the correct entity. Conversely, the second entity 102 must be able to assume that the caller (the first entity 101) is also the one for which it is outputting. Checking authenticity is therefore important in this direction, from the first entity 101 to the second entity 102.

30 **[0062]** Fig. 3 illustrates a processor unit PRZE. The processor unit PRZE comprises a processor CPU, a memory SPE and an input/output interface IOS which ~~[is]~~ **are** used in various ways via an interface IFC. Via a graphics interface, an output is visualized on a monitor MON and/or output on a printer PRT. An input is performed via a mouse MAS or a keyboard TAST. The processor unit PRZE also has a data bus BUS, which ensures the connection of a memory MEM, the processor CPU, and the input/output interface IOS. Furthermore, additional components, for example, additional memory, data memory (hard disk) or scanner, can be connected to the data bus BUS.

35 ~~[List of references:]~~**[0063]** The above-described method and arrangement are illustrative of the principles of the present invention. Numerous modifications and adaptations will be

~~[[1] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks],
DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 42-46.] **ABSTRACT**~~

~~[[2] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks],
DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 73-85.~~

5 ~~[3] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks],
DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 101-117.~~

~~[4] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; <http://csrc.nist.gov/fips/fip180-1.ps>~~

~~[5] NIST, FIPS PUB 81: DES Modes of Operation, December 1980;
<http://www.itl.nist.gov/div897/pubs/fip81.htm>~~

10 ~~[6] A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996,
ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524).~~

Abstract

~~Method and arrangement for authenticating a first entity and a second entity~~

15 ~~[[0064] In order to authenticate a first entity at a second entity, a first number is generated by
[means] way of an asymmetric cryptographic method. This first number is symmetrically encoded and
transmitted to the second entity. The second entity checks the first number by decoding the second
number and thereby authenticates the first entity.~~

SPECIFICATION

TITLE

METHOD AND ARRANGEMENT FOR AUTHENTICATING A FIRST ENTITY AND A
SECOND ENTITY

5 BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The invention relates to a method and an arrangement for authenticating a first entity with a second entity and/or vice versa.

Description of the Related Art

10 [0002] During an authentication, a first entity declares to a second entity reliably that it actually is the first entity. There is a corresponding need in the transmission of (confidential) data to ensure from whom the data actually originate.

[0003] A symmetrical encoding method is known from Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, (Ruland), pages 42-46. In the symmetric encoding method, a key is used both for the encoding and for the decoding. An attacker who comes into possession of such a key can transform a plain text (the information to be encoded) into encoded text, and vice versa. The symmetrical encoding method is also called private key method or method with a
15 secret key. A known algorithm for symmetrical encoding is the DES (data encryption standard) algorithm. It was standardized in 1974 under ANSI X3.92-1981.

[0004] An asymmetrical encoding method is known from Ruland, pages 73-85. In this case, a subscriber is not assigned a single key, but a key system composed of two keys: one key maps the plain text into a transformed one, while the
25 other key permits the inverse operation and converts the transformed text into plain text. Such a method is termed asymmetric because the two parties participating in a cryptographic operation use different keys (of a key system). One of the two keys, for example a key p , can be made publicly known, if the following properties are fulfilled:

30 [0005] - It is not possible to derive from the key p with a justifiable outlay; a secret key s required for the inverse operation.

[0006] - Even if plain text is transformed with the (public) key p , it is not possible to derive the (secret) key s from it.

[0007] For this reason, the asymmetric encoding method is also termed a public key method with a key p which can be made known publicly.

5 [0008] It is possible in principle to derive the secret key s from the public key p . However, this becomes arbitrarily complicated by virtue of the fact, in particular, that algorithms are selected which are based on problems in complexity theory. These algorithms are also spoken of as "one-way trapdoor" functions. A known representative for an asymmetric encoding method is the Diffie-Hellman method A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996, ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524) (Menezes). This method can be used, in particular, for key exchange (Diffie-Hellman key agreement, exponential key exchange).

15 [0009] The term encoding implies the general application of a cryptographic method $V(x,k)$, in which a prescribed input value x (also termed plain text) is converted by means of a secret k (key) into an encoded text $c := V(x,k)$. The plain text x can be reconstructed using knowledge of c and k by means of an inverse decoding method. The term encoding is also understood as "one-way encoding" with the property that there is no inverse, efficiently calculable decoding method.

20 Examples of such a one-way encoding method are a cryptographic one-way function or a cryptographic hash function, for example the algorithm SHA-1, see NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995, available on-line at <http://csrc.nist.gov/fips/fip180-1.ps>.

25 [0010] There is a problem in practice of ensuring that a public key which is used to verify an electronic signature really is the public key of the person who is assumed to be the originator of the transmitted data (ensuring the authenticity of the originator). The public key therefore need not be kept secret, but it must be authentic. There are known mechanisms (see Ruland at pages 101-117) which ensure with a high outlay that the authenticity is reliable. Such a mechanism is the setting up of a trust center, which enjoys trustworthiness and with the aid of which general authenticity is ensured. The setting up of such a trust center, and the exchange of the keys from this trust center are, however, very complicated. For example, it must be ensured during the key allocation that it really is the addressee

[0001]

and not a potential attacker who receives the key or the keys. The costs for setting up and operating the trust center are correspondingly high.

SUMMARY OF THE INVENTION

[0011] It is the object of the invention to ensure authentication without needing
5 to invest in a separate outlay for a certification entity or a trust center.

[0012] This object is achieved according to the discussion below.

[0013] The inventive method for authenticating a first entity with a second
entity is provided in which the first entity carries out an operation $A(x,g)$ on a
(publicly) prescribed known value g and on a value x known only to the first entity.
10 The result of the first operation is encoded with the aid of a first key, which is known
to the first and second entities. The result of the first operation, encoded by way of
the first key, is transmitted by the first entity to the second entity.

[0014] It is particularly advantageous in this case to use a symmetrical
method in order to authenticate one entity in the eyes of a further entity. This
15 authentication is effected without setting up a separate certification entity or a trust
center.

[0015] One refinement consists in that the first operation $A(x,g)$ is an
asymmetric cryptographic method. In particular, the first operation can be carried out
on an arbitrary finite and cyclic group G .

20 [0016] A further refinement consists in that the first operation $A(x,g)$ is a Diffie-
Hellman function $G(gx)$. Alternatively, the first operation can also be an RSA function
 xg .

[0017] A development consists in that the group G is one of the following
groups:

25 [0018] a) a multiplicative group F_q^* of a finite body F_q , in particular having

[0019] a multiplicative group Z_p^* of the integers modulo of a prescribed prime
number p ;

[0020] a multiplicative group F_t^* with $t = 2m$ over a finite body F_t of
characteristic 2; and

[0021] a group of units Z_n^* with n as a composite integer;

[0022] b) a group of points on an elliptic curve over a finite body; and

[0023] c) a Jacobi variant of a hyperelliptic curve over a finite body.

[0024] A further development consists in that the result of the first operation is
5 a second key with which the first entity is authorized to undertake a service on the second entity.

[0025] An additional refinement consists in that the second key is a session key or an authorization associated with an application.

[0026] It also is a development for the second key to be determined in relation
10 to

[0027] $G(gxy)$,

[0028] by virtue of the fact that the second entity carries out an operation $G(gy)$ with a secret number y known only to it. The result of this second operation is encoded with the first key and transmitted to the first entity.

[0029] An additional development consists in that the Diffie-Hellman method
15 is used to generate the second key.

[0030] Another refinement consists in that the encoding is carried out with the first key with the aid of a one-way function, in particular a cryptographic one-way function. A one-way function is distinguished in that it is easy to calculate in one
20 direction, but its inversion can be performed only with so large an outlay that it is impractical. An example of such a one-way function is a cryptographic hash function which generates an output B from an input A. The output B cannot be used to infer the input A, even when the algorithm of the hash function is known.

[0031] Another development is that the encoding which is carried out with the
25 first key corresponds to a symmetrical encoding method.

[0032] A final development is that the transmitted data are confidential data.

[0033] Furthermore, to achieve the object, an authenticating arrangement is specified in which a processor unit is provided which is set up in such a way that

[0034] a) a first entity can carry out a first operation $A(x,g)$ on a prescribed
30 known value g and on a value x known only to the first entity;

[0001] - 4 - SUBSTITUTE SPECIFICATION

[0035] b) the result of the first operation can be encoded with the aid of a first key known to the first and to a second entity;

[0036] c) the result of the first operation encoded with the first key can be transmitted by the first entity to the second entity; and

5 [0037] d) the result of the first operation is decoded by the second entity with the first key, and the first entity can thereby be authenticated.

[0038] This arrangement is particularly suitable for carrying out the method according to the invention or one of its developments explained above.

Brief Description of the Drawings

10 [0039] Exemplary embodiments of the invention are illustrated and explained below with the aid of the drawings.

[0040] Fig. 1 is a block diagram relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case;

15 [0041] Fig. 2 is a block diagram in accordance with fig. 1 and using the DES algorithm; and

[0042] Fig. 3 is a block diagram of a processor unit.

DETAILED DESCRIPTION OF THE INVENTION

20 [0043] Fig. 1 is a diagram relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case. An entity A 101 selects a random number x in a body "mod $p-1$ " (see block 103). The entity 101 now sends an entity 102 a message 104 which has the following format:

[0044] $g, p, T_A, ID_A, gx \bmod p, H(g^x \bmod p, pw, ID_A, T_A, \dots),$

[0045] where

25 x denotes a secret random value of the entity A 101,

y denotes a secret random value of the entity B 102,

g denotes a generator according to the Diffie-Hellman method,

p denotes a prime number for the Diffie-Hellman method,

T_A denotes a time stamp of the entity A during generation and/or transmission of the message,

T_B denotes a time stamp of the entity B during generation and/or transmission of the message,

5 ID_A denotes an identification feature of the entity A,

ID_B denotes an identification feature of the entity B,

$g^x \bmod p$ denotes a public Diffie-Hellman key of the entity A,

$g^y \bmod p$ denotes a public Diffie-Hellman key of the entity B,

10 pw denotes a shared secret between the entities A and B
(password "shared secret"),

$H(M)$ denotes a cryptographic one-way function (hash function) over the parameters M, and

key denotes a session key common to the two entities A and B.

15 [0046] If this message has arrived at the entity 102, a random number y is selected there (see block 105) from the body "mod p-1" and a common key is agreed to in a block 106 as

[0047] $key = g^{xy} \bmod p$.

[0048] The second entity 102 transmits a message 107 with the format

[0049] $T_B, ID_B, g^y \bmod p, H(g^y \bmod p, pw, ID_B, T_B, \dots)$

20 [0050] to the first entity 101. The first entity 101 will then carry out the operation

[0051] $key = g^{xy} \bmod p$

[0052] in a step 108, this likewise yielding the common key "key".

25 [0053] In this case, for example, the body "mod p-1" has been selected as one of many possibilities. Furthermore, the messages 104 and 107 are regarded in each case as one possibility of many. In particular, the fields for addressing within the messages depend on the application and/or the transmission protocol used.

[0054] A cryptographic one-way hash function H is used in Fig. 1. An example for transmitting such a one-way hash function is the SHA-1 algorithm (compare

[0001]

NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; available on-line at <http://csrc.nist.gov/fips/fip180-1.ps>). The use of a symmetrical encoding method, for example the DES algorithm NIST, FIPS PUB 81: DES Modes of Operation, December 1980; available on-line at <http://www.itl.nist.gov/div897/pubs/fip81.htm>, instead of the one-way hash function H , is illustrated in Fig. 2. The blocks 101, 102, 103, 105, 106 and 108 are identical in Fig. 2 to Fig. 1. The message 201 transmitted by the first entity 101 to the second entity 102 has the format

[0055] $g, p, T_A, ID_A, g^x \bmod p, \text{Encr}_{PW}(g^x \bmod p, pw, ID_A, T_A, \dots),$

[0056] where

10 [0057] $\text{Encr}_{PW}(M)$ denotes a symmetrical method for encoding the parameter M with the key PW .

[0058] In the reverse direction, the entity 102 sends the entity 101 in fig. 2 the message 202 which has the following format:

[0059] $T_B, ID_B, g^y \bmod p, \text{Encr}_{PW}(g^y \bmod p, PW, ID_B, T_B, \dots).$

15 [0060] In each case, one message (the message 104 in Fig. 1, and the message 201 in Fig. 2) suffices in order to authenticate the first entity 101 with respect to the second entity 102. Disregarding the fact that the second entity 102, for example, a service to be undertaken within a network connection (for example the Internet) must also be authenticated, it can suffice if only the first entity 101 is
20 authenticated. This already derives after transmission of the respective first messages 104 and 201. If, in particular, the first entity 101 dials in at the second entity 102, it is frequently to be assumed that this second entity 102 is also the correct entity. Conversely, the second entity 102 must be able to assume that the caller (the first entity 101) is also the one for which it is outputting. Checking
25 authenticity is therefore important in this direction, from the first entity 101 to the second entity 102.

[0061] Fig. 3 illustrates a processor unit PRZE. The processor unit PRZE comprises a processor CPU, a memory SPE and an input/output interface IOS which are used in various ways via an interface IFC. Via a graphics interface, an
30 output is visualized on a monitor MON and/or output on a printer PRT. An input is performed via a mouse MAS or a keyboard TAST. The processor unit PRZE also has a data bus BUS, which ensures the connection of a memory MEM, the

[0001]

processor CPU, and the input/output interface IOS. Furthermore, additional components, for example, additional memory, data memory (hard disk) or scanner, can be connected to the data bus BUS.

[0062] The above-described method and arrangement are illustrative of the principles of the present invention. Numerous modifications and adaptations will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.

ABSTRACT

[0063] In order to authenticate a first entity at a second entity, a first number is generated by way of an asymmetric cryptographic method. This first number is symmetrically encoded and transmitted to the second entity. The second entity checks the first number by decoding the second number and thereby authenticates the first entity.

5

Description**Method and arrangement for authenticating a first entity and a second entity**

5

The invention relates to a method and an arrangement for authenticating a first entity with a second entity and/or vice versa.

During an authentication, a first entity
10 declares to a second entity reliably that it actually is the first entity. There is a corresponding need in the transmission of (confidential) data to ensure from whom said data actually originate.

A symmetrical encoding method is known from
15 [1]. In the symmetric encoding method, a key is used both for the encoding and for the decoding. An attacker who comes into possession of such a key can transform a plain text (the information to be encoded) into encoded text, and vice versa. The symmetrical encoding method
20 is also called private key method or method with a secret key. A known algorithm for symmetrical encoding is the DES (data encryption standard) algorithm. It was standardized in 1974 under ANSI X3.92-1981.

An asymmetrical encoding method is known from
25 [2]. In this case, a subscriber is not assigned a single key, but a key system composed of two keys: one key maps the plain text into a transformed one, while the other key permits the inverse operation and converts the transformed text into plain text. Such a
30 method is termed asymmetric, because the two parties participating in a cryptographic operation use different

keys (of a key system). One of the two keys, for example a key p , can be made publicly known, if the following properties are fulfilled:

- 5 - It is not possible to derive from the key p with a justifiable outlay a secret key s required for the inverse operation.
- Even if plain text is transformed with the (public) key p , it is not possible to derive the (secret) key s therefrom.

10 For this reason, the asymmetric encoding method is also termed a public key method with a key p which can be made known publicly.

 It is possible in principle to derive the secret key s from the public key p . However, this
15 becomes arbitrarily complicated by virtue of the fact, in particular, that algorithms are selected which are based on problems in complexity theory. These algorithms are also spoken of as "one-way trapdoor" functions. A known representative for an asymmetric
20 encoding method is the Diffie-Hellman method [6]. This method can be used, in particular, for key exchange (Diffie-Hellman key agreement, exponential key exchange).

 The term encoding implies the general
25 application of a cryptographic method $V(x,k)$, in which a prescribed input value x (also termed plain text) is converted by means of a secret k (key) into an encoded text $c := V(x,k)$. The plain text x can be reconstructed using knowledge of c and k by means of an inverse
30 decoding method. The term encoding is also understood as "one-way encoding" with the property that there is no inverse, efficiently calculable decoding method. Examples of such a one-way encoding method are

a cryptographic one-way function or a cryptographic hash function, for example the algorithm SHA-1, see [4].

There is a problem in practice that it must be
5 ensured that a public key which is used to verify an
electronic signature really is the public key of the
person who is assumed to be the originator of the
transmitted data (ensuring the authenticity of the
originator). The public key therefore need not be kept
10 secret, but it must be authentic. There are known
mechanisms (see [3]) which ensure with a high outlay
that the authenticity is reliable. Such a mechanism is
the setting up of what is called a trust center, which
enjoys trustworthiness and with the aid of which
15 general authenticity is ensured. The setting up of such
a trust center, and the exchange of the keys from this
trust center are, however, very complicated. For
example, it must be ensured during the key allocation
that it really is the addressee and not a potential
20 attacker who receives the key or the keys. The costs
for setting up and operating the trust center are
correspondingly high.

It is the **object** of the invention to ensure
authentication, there being no need to invest in a
25 separate outlay for a certification entity or a trust
center.

This object is achieved in accordance with the
features of the independent patent claims. Developments
of the invention follow from the dependent claims.

30 In order to achieve the object, a method for
authentifying a first entity with a second entity is
specified, in which the first entity

carries out an operation $A(x,g)$ on a (publicly) prescribed known value g and on a value x known only to the first entity. The result of the first operation is encoded with the aid of a first key, which is known to
5 the first and second entities. The result of the first operation, encoded by means of the first key, is transmitted by the first entity to the second entity.

It is particularly advantageous in this case for use to be made of a symmetrical method in order to
10 authenticate one entity in the eyes of a further entity. This authentication is effected without setting up a separate certification entity or a trust center.

One refinement consists in that the first operation $A(x,g)$ is an asymmetric cryptographic method.
15 In particular, the first operation can be carried out on an arbitrary finite and cyclic group G .

A further refinement consists in that the first operation $A(x,g)$ is a Diffie-Hellman function $G(g^x)$. Alternatively, the first operation can also be an RSA
20 function x^g .

A development consists in that the group G is one of the following groups:

- a) a multiplicative group F_q^* of a finite body F_q , in particular having
25 • a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p ;
• a multiplicative group F_t^* with $t = 2^m$ over a finite body F_t of characteristic 2;
• a group of units Z_n^* with n as a composite
30 integer;
b) a group of points on an elliptic curve over a finite body; and

c) a Jacobi variant of a hyperelliptic curve over a finite body.

A further development consists in that the result of the first operation is a second key with which the first entity is authorized to undertake a service on the second entity.

An additional refinement consists in that the second key is a session key or an authorization associated with an application.

It also is a development for the second key to be determined in relation to

$G(g^{xy})$,

by virtue of the fact that the second entity carries out an operation $G(g^y)$ with a secret number y known only to it. The result of this second operation is encoded with the first key and transmitted to the first entity.

An additional development consists in that the Diffie-Hellman method is used to generate the second key.

Another refinement consists in that the encoding is carried out with the first key with the aid of a one-way function, in particular a cryptographic one-way function. A one-way function is distinguished in that it is easy to calculate in one direction, whereas its inversion can be performed only with so large an outlay that this possibility can be neglected in practice. An example of such a one-way function is a cryptographic hash function which generates an output B from an input A . The output B cannot be used to infer the input A ,

even when the algorithm of the hash function is known.

Another development is that the encoding which is carried out with the first key corresponds to a symmetrical encoding method.

5 Finally, it is a development that the transmitted data are confidential data.

 Furthermore, to achieve the object, an authenticating arrangement is specified in which a processor unit is provided which is set up in such a
10 way that

- a) a first entity can carry out a first operation $A(x,g)$ on a prescribed known value g and on a value x known only to the first entity;
- 15 b) the result of the first operation can be encoded with the aid of a first key known to the first and to a second entity;
- c) the result of the first operation encoded with the first key can be transmitted by the first entity to the second entity; and
- 20 d) the result of the first operation is decoded by the second entity with the first key, and the first entity can thereby be authenticated.

 This arrangement is particularly suitable for carrying out the method according to the invention or
25 one of its developments explained above.

Exemplary embodiments of the invention are illustrated and explained below with the aid of the drawing.

In the drawing:

Fig. 1 shows a sketch relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case;

Fig. 2 shows a sketch in accordance with fig. 1 and using the DES algorithm; and

Fig. 3 shows a processor unit.

Fig. 1 is a sketch relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case. An entity A 101 selects a random number x in a body "mod $p-1$ " (see block 103). The entity 101 now sends an entity 102 a message 104 which has the following format:

$g, p, T_A, ID_A, g^x \bmod p, H(g^x \bmod p, PW, ID_A, T_A, \dots),$

where

x	denotes a secret random value of the entity A 101,
y	denotes a secret random value of the entity B 102,
g	denotes a generator according to the Diffie-Hellman method,
p	denotes a prime number for the Diffie-Hellman method,
T_A	denotes a time stamp of the entity A during generation and/or transmission of the message,
T_B	denotes a time stamp of the entity B during generation and/or transmission of the message,
ID_A	denotes an identification feature of the entity A,
ID_B	denotes an identification feature of the entity B,
$g^x \bmod p$	denotes a public Diffie-Hellman key of the entity A,

$g^y \bmod p$ denotes a public Diffie-Hellman key of the entity B,
PW denotes a shared secret between the entities A and B (password "shared secret"),
5 H(M) denotes a cryptographic one-way function (hash function) over the parameters M, and
KEY denotes a session key common to the two
10 entities A and B.

If this message has arrived at the entity 102, a random number y is selected there (see block 105) from the body "mod $p-1$ " and a common key is agreed in a block 106 as

15
$$\text{KEY} = g^{xy} \bmod p.$$

The second entity 102 transmits a message 107 with the format

20
$$T_B, ID_B, g^y \bmod p, H(g^y \bmod p, PW, ID_B, T_B, \dots)$$

to the first entity 101. The first entity 101 will thereupon carry out the operation

25
$$\text{KEY} = g^{xy} \bmod p$$

in a step 108, this likewise yielding the common key KEY.

30 It may be pointed out expressly in this case that, for example, the body "mod $p-1$ " has been selected as one of many possibilities. Furthermore, the messages 104 and 107 are to be regarded in each case as one possibility of many. In particular, the fields for
35 addressing within the messages depend on the application and/or the transmission protocol used.

A cryptographic one-way hash function H is used in fig. 1. An example for transmitting such a one-way hash function is the SHA-1 algorithm (compare [4]). The use of a symmetrical encoding method, for example the DES algorithm [5], instead of the one-way hash function H , is illustrated in **fig. 2**. The blocks 101, 102, 103, 105, 106 and 108 are identical in fig. 2 to fig. 1. The message 201 transmitted by the first entity 101 to the second entity 102 has the format

10

$$g, p, T_A, ID_A, g^x \bmod p, ENC_{PW}(g^x \bmod p, PW, ID_A, T_A, \dots),$$

where

15 $ENC_{PW}(M)$ denotes a symmetrical method for encoding the parameter M with the key PW .

In the reverse direction, the entity 102 sends the entity 101 in fig. 2 the message 202 which has the following format:

20

$$T_B, ID_B, g^y \bmod p, ENC_{PW}(g^y \bmod p, PW, ID_B, T_B, \dots).$$

It may be remarked here, in particular, that in each case one message (the message 104 in fig. 1, and the message 201 in fig. 2) suffices in order to authenticate the first entity 101 with respect to the second entity 202. Disregarding the fact that the second entity 102, for example a service to be undertaken within a network connection, for example the Internet, must also be authenticated, it can suffice if only the first entity 101 is authenticated. This already obtains after transmission of the respective first messages 104 and 201. If, in particular, the first entity 101 dials in at the second entity 102, it is frequently to be assumed that this second

35

entity 102 is also the correct entity. Conversely, the second entity 102 must be able to assume that the caller (the first entity 101) is also the one for which it is outputting. Checking authenticity is therefore
5 important in this direction, from the first entity 101 to the second entity 102.

Fig. 3 illustrates a processor unit PRZE. The processor unit PRZE comprises a processor CPU, a memory SPE and an input/output interface IOS which is used in
10 various ways via an interface IFC. Via a graphics interface, an output is visualized on a monitor MON and/or output on a printer PRT. An input is performed via a mouse MAS or a keyboard TAST. The processor unit PRZE also has a data bus BUS, which ensures the
15 connection of a memory MEM, the processor CPU and the input/output interface IOS. Furthermore, additional components, for example additional memory, data memory (hard disk) or scanner, can be connected to the data bus BUS.

List of references:

- [1] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 42-46.
- [2] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 73-85.
- [3] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 101-117.
- [4] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; <http://csrc.nist.gov/fips/fip180-1.ps>
- [5] NIST, FIPS PUB 81: DES Modes of Operation, December 1980;
<http://www.itl.nist.gov/div897/pubs/fip81.htm>
- [6] A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996, ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524).

Patent claims

1. An authenticating method,
 - a) in which a first entity carries out a first operation $A(x,g)$ on a prescribed known value g and on a value x known only to the first entity, the first operation $A(x,g)$ being an asymmetric cryptographic method;
 - b) in which the result of the first operation is encoded with the aid of a first key, which is known to the first and to a second entity, the encoding being carried out with the first key with the aid of a symmetrical encoding method;
 - c) in which the result of the first operation encoded with the first key is transmitted by the first entity to the second entity; and
 - d) in which the result of the first operation is decoded by the second entity with the first key, and the first entity is thereby authenticated;
 - e) in which the result of the first operation is a second code with which the first entity is authorized to undertake a service on the second entity;
 - f) in which the second key is determined in relation to

$G(g^{xy}),$

by virtue of the fact that the second entity carries out a second operation $G(g^y)$ with a secret number y known only to it, encodes the result of this second operation with the first key and transmits it to the first entity.

2. The method as claimed in claim 1, in which the first operation $A(g, x)$

- a) is a Diffie-Hellman function ($G(g^x)$, $G()$ being an arbitrary, finite cyclic group G ; and
- b) is an RSA function x^g .

3. The method as claimed in one of the preceding claims, in which the first operation is carried out on a group G , the group G being one of the following groups:

- a) a multiplicative group F_q^* of a finite body F_q , in particular having
 - a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p ;
 - a multiplicative group F_t^* with $t = 2^m$ over a finite body F_t of characteristic 2;
 - a group of units Z_n^* with n as a composite integer;
- b) a group of points on an elliptic curve over a finite body; and
- c) a Jacobi variant of a hyperelliptic curve over a finite body.

4. The method as claimed in the preceding claim, in which the second key is a session key or an authorization associated with an application.

5. The method as claimed in one of the preceding claims, in which the Diffie-Hellman method is used to generate the second key.

6. The method as claimed in one of the preceding claims, in which the encoding is carried out with the first key with the aid of a one-way function, in particular a cryptographic one-way function.

7. The method as claimed in one of the preceding claims, in which the transmitted data are confidential data.

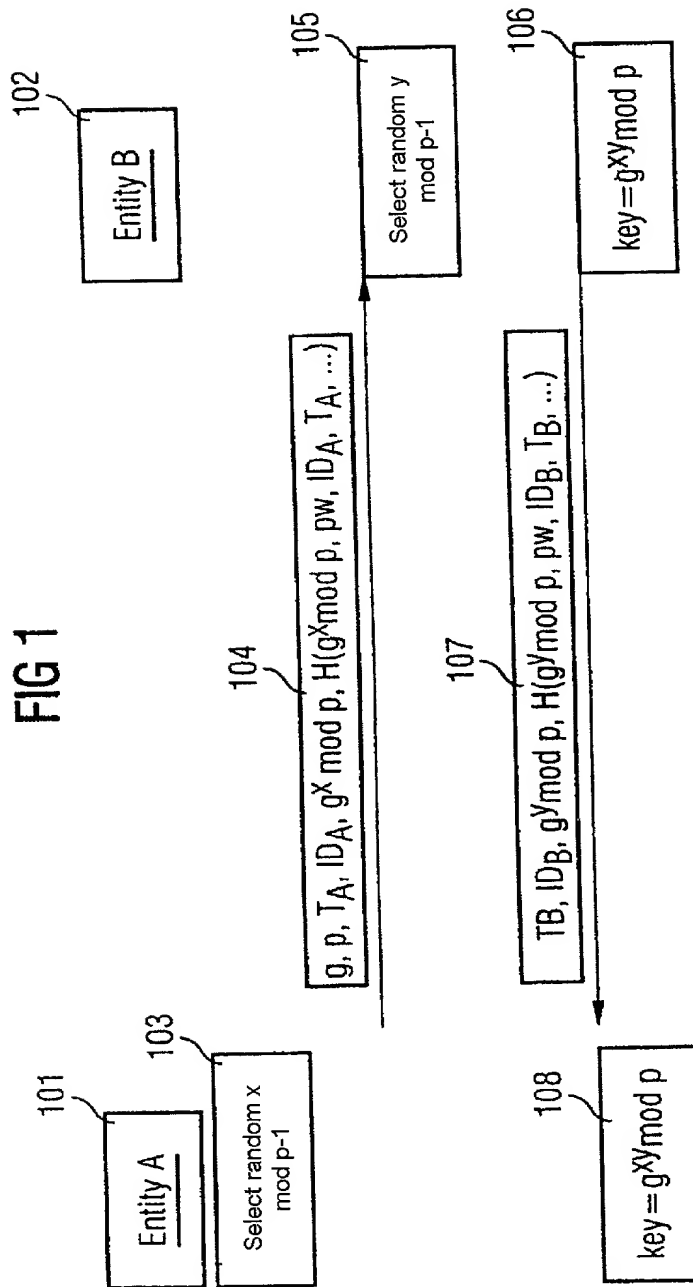
8. An authenticating arrangement in which a processor unit is provided which is set up in such a way that a method as claimed in one of the preceding claims can be carried out.

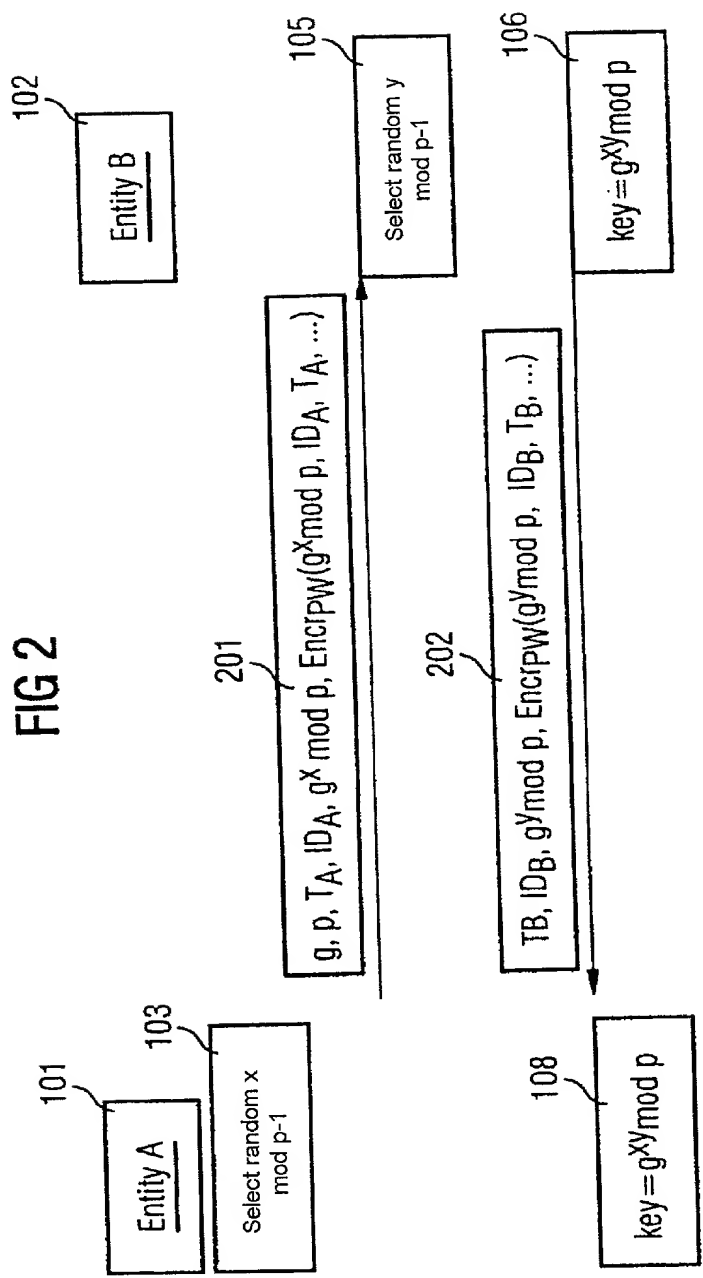
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213

Abstract

Method and arrangement for authenticating a first entity and a second entity

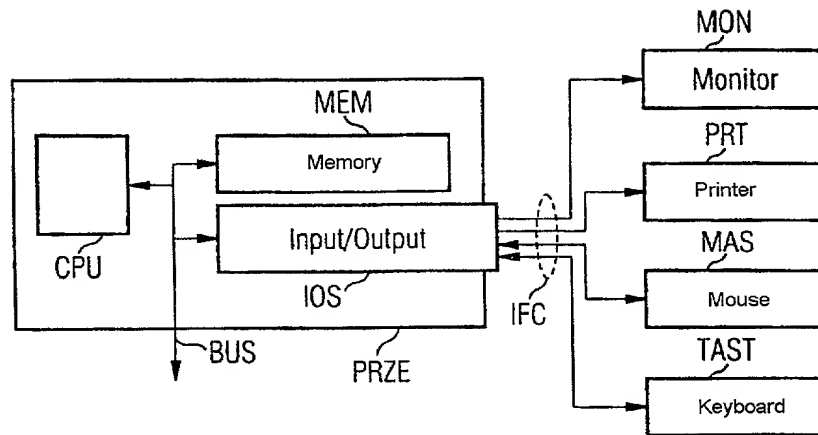
In order to authenticate a first entity at a second entity, a first number is generated by means of an asymmetric cryptographic method. This first number is symmetrically encoded and transmitted to the second entity. The second entity checks the first number by decoding the second number and thereby authenticates the first entity.





3/3

FIG 3



Declaration and Power of Attorney For Patent Application

Erklärung Für Patentanmeldungen Mit Vollmacht

German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Verfahren und Anordnung zur
Authentifikation von einer ersten
Inстанz und einer zweiten Instanz

Method and array for authenticating a
first instance and a second instance

deren Beschreibung

the specification of which

(zutreffendes ankreuzen)

(check one)

☐ hier beigefügt ist.

☐ is attached hereto.

☒ am 11.10.1999 als

☒ was filed on 11.10.1999 as

PCT internationale Anmeldung

PCT international application

PCT Anwendungsnummer PCT/DE99/03262

PCT Application No. PCT/DE99/03262

eingereicht wurde und am _____

and was amended on _____
(if applicable)

abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign applications
Priorität beansprucht

Priority Claimed

19850665.1

DE

03.11.1998

☒

☐

(Number)
(Nummer)

(Country)
(Land)

(Day Month Year Filed)
(Tag Monat Jahr eingereicht)

Yes
Ja

No
Nein

(Number)
(Nummer)

(Country)
(Land)

(Day Month Year Filed)
(Tag Monat Jahr eingereicht)

☐

☐

Yes
Ja

No
Nein

(Number)
(Nummer)

(Country)
(Land)

(Day Month Year Filed)
(Tag Monat Jahr eingereicht)

☐

☐

Yes
Ja

No
Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

PCT/DE99/03262

(Application Serial No.)
(Anmeldeseriennummer)

11.10.1999

(Filing Date D, M, Y)
(Anmeldedatum T, M, J)

(Status)

(patentiert, anhängig,
aufgegeben)

(Status)

(patented, pending,
abandoned)

(Application Serial No.)
(Anmeldeseriennummer)

(Filing Date D,M,Y)
(Anmeldedatum T, M, J)

(Status)

(patentiert, anhängig,
aufgeben)

(Status)

(patented, pending,
abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden können, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: (Name und Registrationsnummer anführen)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Customer No. 26574

And I hereby appoint

Telefongespräche bitte richten an:
(Name und Telefonnummer)

Direct Telephone Calls to: (name and telephone number)

Ext. _____

Postanschrift:

Send Correspondence to:

Schiff, Hardin & Waite
6600 Sears Tower 60606-6473 Chicago, Illinois
Telephone: +1 312 258 5780 and Facsimile +1 312 258 5921

OR
Customer No. 26574

<p>Voller Name des einzigen oder ursprünglichen Erfinders: MARTIN EUCHNER</p>	<p>Full name of sole or first inventor: MARTIN EUCHNER</p>
<p>Unterschrift des Erfinders: <i>Martin Euchner</i> Datum: <i>26.3.2001</i></p>	<p>Inventor's signature: _____ Date: _____</p>
<p>Wohnsitz: MUENCHEN, DEUTSCHLAND <i>DEX</i></p>	<p>Residence: MUENCHEN, GERMANY</p>
<p>Staatsangehörigkeit: DE</p>	<p>Citizenship: DE</p>
<p>Postanschrift: LORENZSTR. 2</p>	<p>Post Office Address: LORENZSTR. 2</p>
<p>81737 MUENCHEN</p>	<p>81737 MUENCHEN</p>
<p>Voller Name des zweiten Miterfinders (falls zutreffend):</p> <p>Full name of second joint inventor, if any:</p> <p>Unterschrift des Erfinders: _____ Datum: _____</p> <p>Second Inventor's signature: _____ Date: _____</p> <p>Wohnsitz: _____</p> <p>Residence: _____</p> <p>Staatsangehörigkeit: _____</p> <p>Citizenship: _____</p> <p>Postanschrift: _____</p> <p>Post Office Address: _____</p>	

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).